Data Sheet

NCP Secure Enterprise Management

SECURE COMMUNICATIONS

Next Generation Network Access Technology

Centrally Managed VPN – fully Automatic Operation of a Remote Access VPN via a Single Console

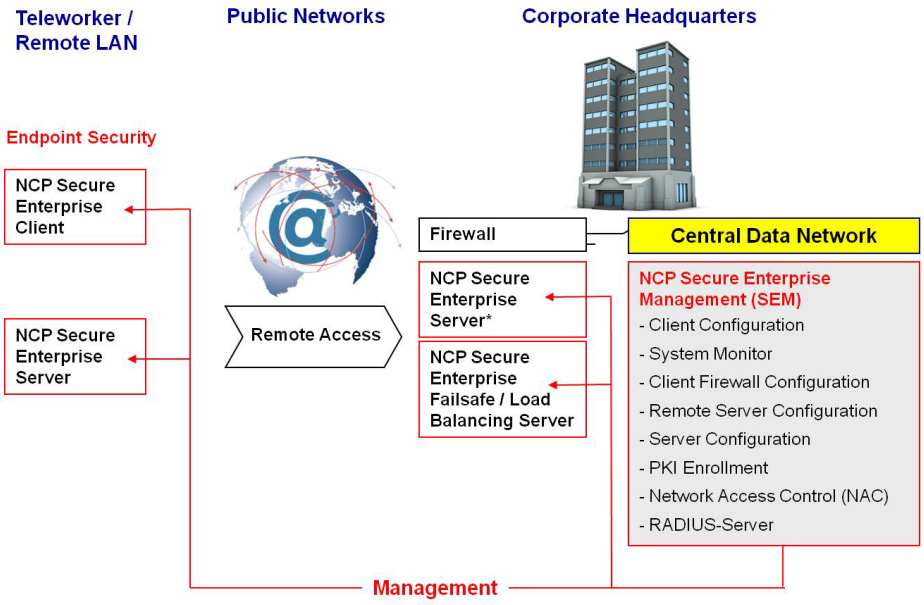
- **Enables easy rollout and operation of secure remote access infrastructures**
- **Central creation of client configuration**
- **Configuration changes on the fly**
- **Minimal management effort**
- **Less help-desk calls**
- **Little training and documentation effort**
- **Integration into any existing IT infrastructure**
- **More than 25 years of remote access expertise**
- **Integrated RADIUS Server**

Overview

NCP has been focusing on developing innovative software for more than 25 years. It aims to support companies and authorities with secure remote access which is easy to establish and operate. In this, NCP's Secure Enterprise Management (SEM) is an important component, so to say, the *heart* of NCP's Next Generation Network Access Technology.

Fully Automatic Operation

NCP's Secure Enterprise Management can be connected with the company's existing user management (e.g. Microsoft Active Directory) and request regular updates. As soon as a new employee is listed in this data base SEM creates an individual configuration for this user, according to defined templates, enters it at the RADIUS server and, among others, assigns a provider



* You can integrate VPN gateways of third-party suppliers into a managed VPN environment. This, however, restricts the use of some SEM features.

recognition and a software certificate. If a former employee has been removed from the data base, SEM immediately blocks this VPN access. This eliminates the need to manually configure the computers of all mobile employees. SEM also enables fast rollout of a large number of users or a software certificates.

Components

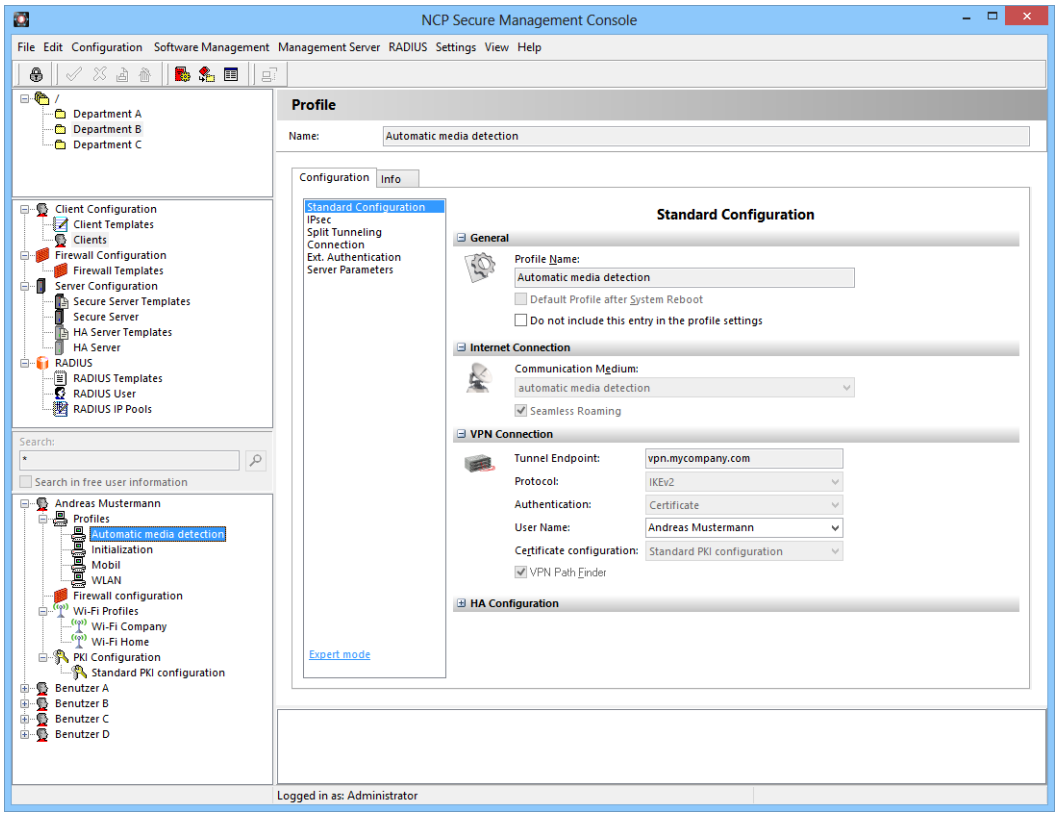
NCP Secure Enterprise Management consists of the Management Server and the Management Console with graphic user interface. The Management Server serves for configuration and management of all connected NCP components. This includes the NCP Secure Enterprise Clients for Windows, Mac OS, Android, Linux and CE/Windows Mobile as well as the NCP Secure Enterprise VPN Server. The Management Server is a database-based system and it corresponds with virtually any database via ODBC (e.g. Oracle, MySQL, MS SQL, MS Access, MaxDB). Optionally the Backup Management Server ensures high-availability of the Management Server, which always has the current data repository available through an integrated replication service.

- Management Server Plug-ins:
- Client Configuration
- System Monitor
- Client Firewall Configuration
- Server Configuration
- Remote Server Configuration
- Network Access Control (NAC), PKI Enrollment, RADIUS

All configuration parameter are stored in the database and usually included into the backup process of the VPN operator. The Management Console can be installed at various administrator work stations, which require a network connection to the Management Server.

Client Configuration Plug-in

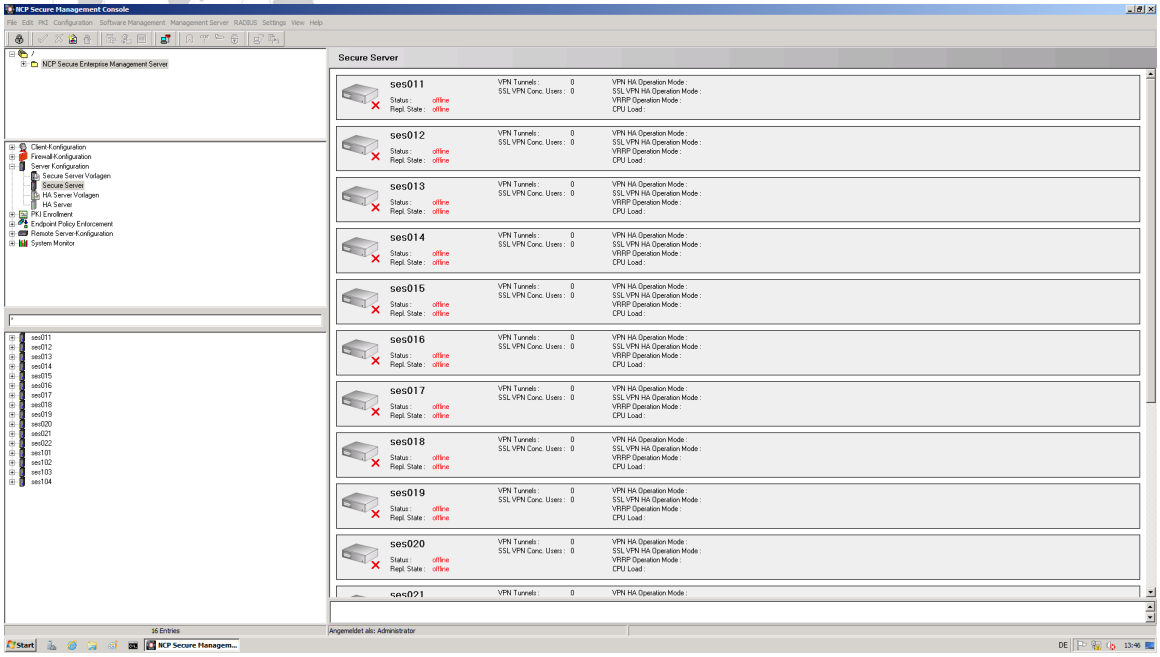
This plug-in enables configuration and administration of NCP Secure Enterprise Clients. All relevant parameters are predefined and stored in templates.



NCP Secure Management Console: Client Configuration

Automatic Update Process

The fully automatic update process allows the administrator to centrally provide all remote NCP Enterprise Clients with configuration and certificate updates. As soon as the client logs in to the corporate network next, the system automatically installs them on the client. If malfunctions occur



NCP Secure Management Console: Monitoring

during the transmission, then the previously existing configuration remains unaffected. The software is only updated after complete error-free transmission of all pre-defined files. An encrypted VPN Tunnel secures data transmission. As long as the end device is within the corporate network, the client can be updated without a VPN connection. If a NCP Secure Enterprise Client for Windows is used, the administrator can bind the client software update to the communication medium.

The NCP Management Console enables interactive input or transfer of all relevant data; alternatively this can be done in a script-driven process. For rollout, for example, the administrator can automatically transfer user data, license keys, provider passwords, etc. to the Management Server for each remote system (= managed unit). As VPN gateway, you can use the NCP Secure Enterprise VPN Server or the VPN Gateway of any third party producer (see compatibility list at www.ncp-e.com).

License Management Plug-in

The licenses of all connected components are centrally stored at the NCP Secure Enterprise Management Server. The system transfers them into a license pool and automatically manages them according to specified guidelines. This license transfer might be used for: transfer into a configuration per remote client or gateway, returning the license to the license pool when an employee leaves a company, or triggering a prompt when no more licenses are available.

System Monitor Plug-in

This plug-in provides fast information in form of bar graphs or line diagrams about all important events within a VPN installation. The administrator can use the system monitor as needed to call up current status information in real time, or to access previously saved data repositories of the remote access environment.

Client Firewall Configuration Plug-in

The NCP Secure Client software has a centrally managed, integrated Personal Firewall. The Client Firewall Configuration plug-in enables to granularly adjust the firewall rules for each teleworkstation.

Remote Server and Server Configuration Plug-in

The Remote Server Configuration plug-in enables configuration, management and licensing of remote gateways as managed units, for example in branch offices. It is used for configuration and management of Secure Servers (Secure Enterprise VPN Server and Secure High Availability Server) of the central network. The administrator uses the management console to manage the access rights to each server and to create the server configuration. The console allows the administrator to use templates for a group of servers (server farm) and for client user groups.

PKI Enrollment Plug-in

The PKI Enrollment plug-in functions as Registration Authority (RA) and manages the creation as well as the administration of electronic certificates (X.509 v3) in conjunction with different Certification Authorities (CA). A generated certificate can optionally be stored as soft certificate (PKCS#12) or on hardware, e.g. smart card or USB token (PKCS#11). The NCP Demo CA that ships with the product can be used to simulate a PKI during the test phase, however, it is not intended for productive use. Conversion to an external CA is problem-free.

Network Access Control Plug-in (Endpoint Security)

Through endpoint security - also known as Network Access Control Plug-in - the system checks all security relevant parameters of the device prior to access to the company network. Some of these parameters are: state of virus scanner, information about services, content of certificates or software version. Through these checks each end-device is compelled to meet the security policies and the user can neither avoid nor manipulate them. If a device does not comply to these policies, it is led into a designated quarantine zone (when configured).

Parameter Lock

The parameter locks of the NCP Secure Clients have two main functions: The first is to reduce the complexity of configuration possibilities. This function hides parameter folders for features which are not used, so that the user only sees the settings which are relevant for his working environment. The second function is that pre-settings can be made which the user cannot change. This avoids misconfigurations and undesired connection set ups.

RADIUS Plug-in

This plug-in is used to manage the integrated RADIUS server and to combine existing RADIUS Servers i.e. replace them in an economic way.

Advanced Authentication Add-On

Through this add-on selected users receive a pass code as SMS (text message) on their cell phone. Then they have to additionally enter this pass code during authentication at the client (two-factor authentication). A random generator of the Secure Enterprise Management creates this pass code at each connection setup to the company network.

The system then sends the SMS (text message) to the user who, in a first step, has authenticated towards the SEM by entering his VPN access data.

Multi Company Support

Multi-company support makes Secure Enterprise Management a natural choice for implementation at Managed Security Service Providers (MSSP), in cloud environments, or in remote access structures, where multiple companies jointly use one VPN platform (VPN sharing). This is done by forming groups and using a convenient method of assigning rights. Administrators are created in such a manner that each has exclusive access to his area, in other words to the units that he is responsible for managing. The possibility of encroaching on data of other clients in their protected areas is excluded.

Technical Data

System Requirements

Operating Systems	Management Server: 32-Bit: Windows 2003 Server, Windows 2003 R2, Windows Server 2008; Linux Kernel 2.6 as of Version 2.6.16 (distributors on request) 64-Bit: Windows Server 2008, Windows Server 2008 R2; Linux Kernel 2.6 as of Version 2.6.16 (distributors on request)
Managed Units	Secure Enterprise Client as of V 9.1; Secure Android Client as of V 2.32 Secure Enterprise Server as of V 8.0
Plug-ins	Automatic Update, Client Firewall Configuration, Client Configuration, Endpoint Policy Enforcement, License Management, PKI, RADIUS, Remote Server Configuration, Server Configuration, Script and System Monitor
Network Access Control (Endpoint Security)	Endpoint Policy Enforcement for incoming data connections. Verification of predefined, security-relevant client parameters. Measures in the event of target/actual deviations in IPsec VPN: ‣ Disconnect or continue in the quarantine zone with instructions for action (Message box) or start of external applications (e.g. virus scanner update), logging in Log files Measures in the event of target/ actual deviations in SSL VPN: ‣ Individual grading of access authorization to certain applications in accordance with defined security levels.
Advanced Authentication	SEM 3.00 with license 3.0; Advanced Authentication Add-On; Client Plug-in 9.30 as of Build 50 (required setting of product configuration: 9.3); RADIUS Plug-in as of 2.06 Build 4
Multi Company Support	Group capability; support of max. 256 domain groups (i.e. configuration of: authentication, forwarding, filter groups, IP pools, bandwidth limitation, etc.)
User Administration	LDAP, Novell NDS, MS Active Directory Services
Databases	Oracle as of Version 9.0; MySQL as of 4.x, 5.0 and 5.1; Microsoft SQL Server 2000 - 2008
Statistics and Logging	Detailed statistics, logging functionality, sending SYSLOG messages
IF-MAP	The overall aim of the ESUKOM Project is the design and development of a real time security solution for company networks which works on the basis of consolidating meta data. The special focus of the project is the threat resulting from mobile end devices, e.g. smartphones. ESUKOM focuses on the integration of existing security solutions (commercial and open source) which are based on a consistent meta data format according to IF-MAP specifications of the Trusted Computing Group (TCG). The IF-MAP server of the Hannover University of Applied Science and Arts can currently be used for free-of-charge testing. The URL is: http://trust.f4.hs-hannover.de/
Client/User Authentication Processes	OTP token, certificates (X.509 v.3): User and hardware certificates (IPsec), user name and password (XAUTH)

Certificates (X.509 v.3)

Server Certificates	It is possible to use certificates which are provided via the following interfaces: PKCS#11 interface for encryption tokens (USB and smart cards); PKCS#12 interface for private keys in soft certificates
Revocation Lists	Revocation: EPRL (End-entity Public-key Certificate Revocation List, formerly CRL), CARL (Certification Authority Revocation List, formerly ARL),
Online Check	Automatic downloads of revocation lists from the CA at certain intervals; Online check: Checking certificates via OCSP or OCSP over http
Certification Authorities	Microsoft Certificate Services: as „stand alone CA": as of Windows 2000 Server; as "integrated CA in the domain": as of Windows 2000 (certificate templates cannot be adapted) as of Windows 2003 Enterprise Server

Virus Scanner	Windows 8/7, Windows Vista and Windows XP SP2 allow the system to request all virus scanner which deliver their status over WMI (Windows Management Instrumentation) or NAC (Network Admission Control) to the Security Center.
Supported RFCs and Drafts	RFC 2138 Remote Authentication Dial In User Service (RADIUS); RFC 2139 RADIUS Accounting; RFC 2433 Microsoft CHAP; RFC 2759 Microsoft CHAP V2; RFC 2548 Microsoft Vendor-specific RADIUS Attributes; RFC 3579 RADIUS Support For Extensible Authentication Protocol (EAP); RFC 2716 PPP EAP TLS Authentication Protocol; RFC 2246 The TLS Protocol; RFC 2284 PPP Extensible Authentication Protocol (EAP); RFC 2716 Certificate Management Protocol; RFC 2511Certificate Request Message Format; Draft-ietf-pkix-cmp-transport-protocols-04.txt Transport Protocols for CMP; Draft-ietf-pkix-rfc2511bis-05.txt Certificate Request Message Format (CRMF)

Recommended System Requirements

Computer	512 MB System Memory; CPU mind. Pentium III-800 MHz (depending on number of managed units); With RADIUS Plug-in: Pentium IV-1,5 GHz; hard drive: min. 50 MB of free memory plus memory for log files and ca. 20 MB per software packet

Recommended VPN Clients / Compatibilities

NCP Secure Enterprise Clients	Windows 32/64, Mac OS X, Windows Mobile, Android, Windows CE, Linux,
Third Party VPN Clients	iOS

Recommended System Requirements*

Number of Concurrent Users	**Computer**
1-100 Concurrent User	CPU: Intel Dual Core 1,83 GHz or comparable x86 Processor, 1024 MB RAM
200+ Concurrent User	CPU: Intel Dual Core 1,83 GHz or comparable x86 Processor, 1024 MB RAM